CLAIMS

What is claimed is:

1. A method for making a secure identification information member for a user comprising:

generating one or more obscured user identifiers; and

generating a translucent identification member having a translucent area that includes the one or more obscured user identifiers.

2. The method of claim 1 wherein generating the one or more obscured user identifiers includes:

obtaining user specific information associated with the user; and

combining the user specific information with other information to produce the one or more obscured user identifiers.

3. The method of claim 1 wherein generating the one or more obscured user identifiers includes:

obtaining user specific information associated with the user; and

using the user specific information to produce the one or more obscured user identifiers.

4. The method of claim 1 wherein generating the one or more obscured user identifiers includes:

generating the one or more obscured user identifiers independent of any user specific information.

5. The method of claim 1 including:

assigning identification information to the one or more obscured user identifiers;

storing the identification information and associated one or more obscured user identifiers; and

providing the identification information on the translucent identification member.

6. An apparatus for creating an apparatus for securely providing identification information comprising:

an issuer operative to generate one or more obscured user identifiers; and operative to generate a translucent identification member having a translucent area that includes the one or more obscured user identifiers.

7. The apparatus of claim 6 wherein the issuer is operative to obtain user specific information associated with a user; and combine the user specific information with other information to produce the one or more obscured user identifiers.

8. The apparatus of claim 6 wherein the issuer is operative to obtain user specific information associated with a user and use the user specific information to produce the one or more obscured user identifiers.

9. The apparatus of claim 6 wherein the issuer is operative to generate the one or more obscured user identifiers independent of any user specific information.

10. The apparatus of claim 6 wherein the issuer is operative to assign identification information to the one or more obscured user identifiers; store the identification information and associated one or more obscured user identifiers; and provide the identification information for placement on the translucent identification member.

11. A method for securely providing identification information comprising:

sending a visual filtering pattern to a display device wherein the filtering pattern is defined such that when the visual filtering pattern is visually combined with one or more

obscured user identifiers located on a translucent identification member, a designated one of the one or more identifiers is visually revealed; and

receiving data representing the visually revealed identifier.

12. The method of claim 11 including sending the received data representing the visually revealed identifier to an authentication apparatus.

13. The method of claim 11 wherein the data representing the visually revealed identifier is received using a device other than the device on which the visual filtering pattern is displayed.

14. A method for securely providing identification information comprising:

receiving user identification information;

using the user identification information to identify a translucent identification member and one or more obscured user identifiers known to have been associated with such user;

selecting from the one or more obscured user identifiers a particular obscured user identifier to be used as a second factor of authentication for the user associated with the received user identification information;

generating a visual filtering pattern that when combined with the one more obscured user identifiers on the identified translucent identification member will reveal the selected particular obscured user identifier from among the obscured user identifiers;

transmitting the visual filtering pattern and requesting entry of the revealed identifier; and

receiving data representing the revealed identifier.

15. The method of claim 14 including examining the received data representing the visually revealed identifier to determine if it matches an expected value.

16. The method of claim 15 wherein the expected value has been determined before receipt of the received data representing the visually revealed identifier.

17. The method of claim 15 wherein the expected value is determined after receipt of the received data representing the visually revealed identifier.

18. The method of claim 15 including granting a right to the user if the received data representing the visually revealed identifier matches the expected value.

19. The method of claim 15 including sending the received data representing the visually revealed identifier to an authentication apparatus.

20. The method of claim 19 including receiving a reply from the authentication apparatus and granting a right to the user if the authentication apparatus indicates that a match with the expected value occurred.

21. The method of claim 15 wherein the step of using the user identification information includes checking if the translucent identification member is valid based on a list of invalid translucent identification members.

22. A method for associating secure identification information with a user comprising:

receiving a request from a user for one or more obscured user identifiers;

recording a link between the user and the identification information associated with the one or more obscured user identifiers.

23. The method of claim 22 including:

providing the one or more obscured user identifiers to the user.

24. The method of claim 23 wherein the one or more obscured user identifiers are on a translucent identification member that is sent to the user.

25. The method of claim 23 wherein the one or more obscured user identifiers are sent to a third party to be placed on a translucent identification member for the user.

26. The method of claim 23 wherein the one or more obscured user identifiers are sent to the user for placement on a translucent identification member.

27. The method of claim 22 wherein the one or more obscured user identifiers are selected from a pre-existing pool of obscured user identifiers.

28. The method of claim 22 wherein the request from the user includes user specific information and wherein the user specific information is combined with other information to produce the one or more obscured user identifiers.

29. A system for securely providing identification information comprising:

a circuit operative to receive user identification information;

a circuit operative to use such user identification information to identify a translucent identification member and one or more obscured user identifiers known to have been associated with such user; and for selecting from the one or more obscured user identifiers a particular obscured user identifier to be used as a second factor of authentication for the user associated with the received user identification information;

a circuit for generating a visual filtering pattern that when combined with the one more obscured user identifiers on the identified translucent identification member will reveal an expected revealed identifier from among the obscured user identifiers;

a circuit for transmitting the visual filtering pattern and for requesting entry of a revealed identifier; and

a circuit for receiving data representing the revealed identifier.

30. The system of claim 29 including a circuit to examine the received data representing the revealed identifier to determine if it matches the expected revealed identifier.

31. The system of claim 30 wherein the circuit for examining the received data can determine the expected revealed identifier prior to the receipt of the received data representing the revealed identifier.

32. The system of claim 30 wherein the circuit for examining the received data can determine the expected received identifier after the receipt of the received data representing the revealed identifier.

33. The system of claim 30 including a circuit to grant a right to the user if the received data representing the revealed identifier matches the expected revealed identifier.

34. The system of claim 30 wherein the circuit for examining the received data representing the revealed identifier does so by sending the received data to an authentication device.

35. The system of claim 34 including a circuit for receiving a reply from the authentication device and for granting a right to the user if the authentication device indicates that a match with the expected revealed identifier occurred.

36. An apparatus for securely providing identification information comprising:

a translucent identification member authenticator operative to receive user data representing a revealed identifier in response to overlaying a translucent identification member on a display; and operative to compare the received data with a corresponding expected revealed identifier to determine whether proper authentication of the user is appropriate.

37. The apparatus of claim 36 wherein the translucent identification member authenticator determines the expected revealed identifier prior to the receipt of the received data corresponding to the revealed identifier.

38. The apparatus of claim 36 wherein the translucent identification member authenticator determines the expected revealed identifier after the receipt of the received data corresponding to the revealed identifier.

39. An apparatus for associating secure identification information with a user comprising:

a circuit operative to receive a request from a user for a translucent identification member; and operative to record a link between the user and the identification information associated with the one or more obscured user identifiers.

40. The apparatus of claim 39 wherein the circuit is operative to select the one or more obscured user identifiers are selected from a pre-existing pool of one or more obscured user identifiers.

41. The apparatus of claim 39 wherein the circuit is operative to request information from the user that includes user specific information and wherein the user specific information is combined with other information to produce the one or more obscured user identifiers.

42. The apparatus of claim 39 wherein the circuit is operative to request information from the user that includes user specific information and wherein the user specific information is used to produce the one or more obscured user identifiers.

43. An apparatus for securely providing identification information comprising:

a visual filtering pattern generator operative to generate a visual filtering pattern based on data identifying a translucent identification member that has a translucent area that

includes one or more obscured user identifiers such that when the visual filtering pattern is visually combined with the one or more obscured user identifiers on the translucent identification member, a designated one of the one or more obscured user identifiers is revealed.

44. The apparatus of claim 43 including a translucent identification member authenticator operative to receive data representing the revealed identifier in response to overlaying the translucent identification member with one or more obscured user identifiers on a display; and to compare the received data with a corresponding expected identifier to determine whether proper authentication of the recipient is appropriate.

45. A method for securely providing identification information comprising:

displaying a visual filtering pattern defined such that when the visual filtering pattern is combined with one or more obscured user identifiers located on a translucent identification member, a designated one of the one or more visual identifiers is revealed; and

receiving input data representing the visually revealed identifier.

46. The method of claim 45 wherein displaying the visual filtering pattern includes indicating an overlay area on the display for overlaying the translucent identification member.

47. The method of claim 46 including the step of transmitting the received input data representing the visually revealed identifier.

48. The method of claim 45 wherein the received input data is received on a device other than the device that is used to display the visual filtering pattern.

49. A secure identification information member comprising:

a translucent area having an information pattern representing one or more identifiers configured to overlay at least a portion of a display screen.

50. The secure identification information member of claim 49 including additional information thereon relating to at least one specific use of the member.

51. The secure identification information member of claim 49 wherein the additional information represents information for use in at least one of: voting, banking, online transaction and membership.

52. A transaction card comprising:

a first portion at least containing transaction card identification information; and

a second portion containing a translucent identification member having a translucent area that includes one or more obscured user identifiers.

53. The transaction card of claim 52 wherein the second portion containing the translucent identification member includes an attached translucent identification member.

54. The transaction card of claim 52 wherein the second portion containing the translucent identification member includes an open area with a connecting structure configured to receive and hold the translucent identification member.

55. The transaction card of claim 52 wherein the translucent identification member is configured to overlay at least a portion of a display screen.

56. The transaction card of claim 52 wherein the translucent identification member includes a translucent area having an information pattern representing a plurality of different identifiers for use at a plurality of different times and is configured to overlay at least a portion of a display screen.